Ethical Problems of Smart Wearable Devices

Victor Chang[1][a], Xin Xu[1], Barbara Wong[2] and Victor Mendez[3]
[1]*International Business School Suzhou, Xi'an Jiaotong-Liverpool University, Suzhou, China*
[2]*Department of Industrial Design, Xi'an Jiaotong-Liverpool University, Suzhou, China*
[2]*Universitat Autònoma de Barcelona, UAB, Spain*
{Victor.Chang, Barbara.Wong}@xjtlu.edu.cn, Xin.Xu18@student.xjtlu.edu.cn , victor.mendez@uab.es

Keywords: Big data, Wearable devices, ethical issues

Abstract: With usage of big data and development of advanced technology, smart wearable devices have come to market with multifunction. The wearables include smart watches, smart bands, smart glasses and so on. The big data and data analysis can provide more benefits for users and companies. As for users, smart wearables can help to provide a more convenient and healthier lifestyle. Besides, the big data can provide more support for decision making of companies and may encourage creativity. However, ethical problems also appear with the development of smart wearables. First, vulnerabilities of system can be found, which may pose potential threat to users. Second, misused data will also cause bad influence and the companies should be more transparent on the usage of personal data. Third, some smart wearable companies take priority of multifunction of devices rather than data safety. Based on these problems, different entities should take on responsibilities. Users should improve their awareness and knowledge to protect their personal data. As for companies, some principles of personal data released by OECD can be applied when companies deal with personal information. When it comes to society, supervisions of the industry and support for advanced technology should be carried out.

1 INTRODUCTION

With the development of smart technology, big data produces great value in economy as well as daily life. Cloud computing can gather the big data and conduct algorithms to realize the automated control over facilities. Data analytics by different methodology like linear regression and sequence analysis can be carried out to figure out related factors. Moreover, the global needs of smart wearable devices have been on the way up (Mukhopadhyay, 2015). The combination of data analytics and functions of wearables have stimulated the market and smart control systems will improve efficiency. However, challenges have existed in big data. Chen et al., (2013) have illustrated that data variety still be difficult problems and utilization of information keeps at a low level. Another challenge is data safety. Data safety has requirement for different entities in the chain covering technology development and regulations from organizations.

In 2017, Germany announced a ban on sales of children's smart watches. The main reasons for the ban is that the smart watch can be monitored by hackers, since the smart watch can be a tool for threatening children's safety (Filip, 2017). The announcement was also a warning for wearers of smart wearable devices. The devices are used as mini smart phones recording activities of health. The sensors of different smart wearable device cover data of many aspects about physical quality indexes. However, system vulnerabilities can be accessed by attackers (Do et al., 2016). Therefore, for some unsafe devices, the more data wearables collect, the more threats users will have. If security concern is neglected, it may cause more security problems as technology develops further. This paper will give an overview of big data and big data analytics in smart wearable device industry. The ethical issues raised by usage of big data will be concluded. Based on the ethical problems, some suggestions of these ethical problems will be discussed.

[a] https://orcid.org/0000-0002-8012-5852

2 BACKGROUND

The smart wearable devices are the application of smart technology based on traditional wearable devices. People can enjoy multifunction and basic functions of traditional wearables. For example, smart watch supports functions of making calls, health monitoring and presenting time. Nowadays, smart wearable devices contain smart watches, smart bands, smart glasses and so on. Based on the data from www.chyxx.com and Zhiyan.org, the market scale of smart wearable devices in China has increased consistently. The following figure shows the trend in recent years.

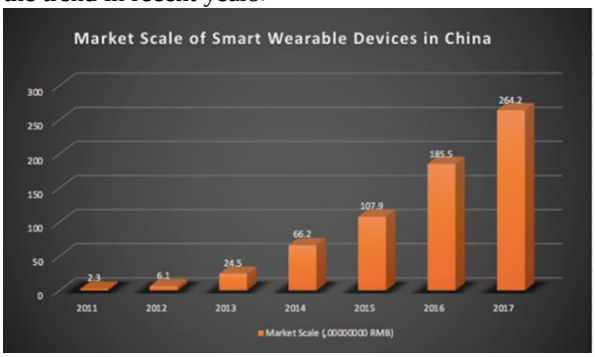

Figure 1: Market scale of smart wearable devices in China

According to the data from www.chyxx.com and Zhiyan.org, the trend has shown rapid development of the industry and its growth rate reached the peak in 2013 and 2014. The growth rate has slowed down after that. The market scale in China has reached 26.42 billion RMB in 2017. Furthermore, according to the report of Strategy Analytics (2018), the shipment of smart watch in the world in Q3 of 2018 has reached 10 million and increased by 67% year-over-year (Mawston, 2018). Therefore, the market has a positive potential due to the increasing usage of advanced technology.

The calculation function of watches appeared in the 1940s. Since then, different programs have been developed on the devices. The first smart watch operating Linux was introduced by IBM in 2000 (Edwards, 2013). Although battery life and small memory of the device cannot support sophisticated functions, many people consider it can represent a great advance of smartwatch. Functions like sensors and Bluetooth can be supported on it. As potential of smart watch market is tapped, smart watch of Samsung, LG G watch and Apple watch have been launched subsequently (Kastrenakes, 2014).

Apart from smart watch, the smart band is another important component of wearable devices, which were launched by the first programmable band Japanese Seiko. Jawbone UP has been introduced in 2011 with features of sleeping monitor. Then, Fitbit Flex was put into market by Fitbit in 2013 pioneered data sharing of the smart band. Since 2014, more smart bands have been introduced to market like Talk band B1 of Huawei and Microsoft bands (Zaker, 2017). More functions have been supported in smart bands to lead to a better lifestyle of users.

Smart glasses combine smart technology and traditional glasses. Through mobile connection network, it can support functions like taking pictures, videos, video calls and so on. In 2012, Google introduced the design and development plan of the first smart glass named “Project Glass” (Techopedia, 2018). It operates on Android and contains functions of most smart phone. The smart glasses also have potential in industry. Realwear has introduced HMT-1Z1 as commercial wearable devices for security. By limiting electrical energy and thermal energy to guarantee secure operation of equipment (Realwear, 2018). Although smart glass market is in the primary stage of development, the popularizing rate and shipment may increase in future with the progress of smart city.

With the emergence of new wearables, standardization will be the global trend for wearable industry. For example, different RFID standards systems have been introduced by organizations for manufacturers in the industry and benefit for supply chain (Impinj, 2019). However, the implementation of the standards in different countries has to apply to different market. According to the research about RFID on medical devices (Dong et al., 2016), the mismatching between technical requirement and mainstream standards still exist in medical devices. Since RFID technology in medical devices is at primary stage, the problems need more attentions and the reduction of unstandardized products need measurements from regulators in a long term.

3 SMART WEARABLE DEVICES AND BIG DATA

3.1 Data Sources

Compared with traditional devices, data and data analysis of smart wearable devices are the main difference. Data source of smart wearable devices contains mobile communication data, private data and data from sensors (KaraKaya et al., 2016). For example, data of pedometer are a combination of

sensors in wearables and data algorithm (Jayalath & Abhayasinghe, 2013). Pace account can be calculated and the data can be stored by wearables and acceleration sensors can measure quality of sleep by monitoring the movement of wrist. Therefore, data of different activities in wearables can be analysed through different algorithms.

3.2 Model of Smart Wearable Devices

The development of wearable device is closely connected with big data. Every wearer becomes a creator of big data and big data are collected from different areas of wearer's daily life. Wu et al., (2017) have illustrated architecture of system. Based on the system, wearable devices can be divided into different entities to transmit and store data. In this section, the following entities can support the main functions of smart wearable devices.

Sensors in smart wearable devices mainly installed to collect data relating to health of wearers. An et al.,(2017) have indicated the differentiation of sensors which can be divided into individual sensors, multiplexed sensors and wireless sensors. Multiplexed sensors can also sense the external environment. The accuracy of data collected by the sensors can show the physical status. Therefore, the accuracy of sensors should keep stable and reliable for further analysis.

The Bluetooth can connect with smart phone in a short distance and complete the data transmission. Do et al., (2016) have explained the smart phone running Android can support tasks with internet on wearable devices via the Bluetooth. However, the Bluetooth pairing requires the access from wearers. In other words, the connection supports operation of functions on wearables but also leads to vulnerabilities. In addition to Bluetooth, NFC is short-range radio technology based on RFID and interconnection technology and supports data exchange with compatible devices. It mainly supports payment and provides convenience for people's outgoing. For example, NFC technology can support the payment of taking public transport (Ondrus & Pigneur, 2007).

Wu et al., (2017) have explained the role of App on connection between sensors and Bluetooth. The Apps on the smart phone support the Bluetooth pairing between the two devices. From another perspective, it will increase the difficulty in the management of personal data on different devices.

Cloud service is widely used for data storage in smart wearable devices. Li et al., (2014) have explained that through clustered application and distributed file system, cloud can provide data storage through application software in different devices.

3.3 Big Data Analytics and Its Benefits to Smart Wearable Device

Compared with traditional wearable devices, smart wearable devices have more advanced functions and are supported by big data. The majority of smart watches contain functions like calls, messages, health information tailoring and so on. Personal information set by users on different Apps can provide convenience of operations to customers. Relying on the close connection between smart wearable devices and smart phones, wearables can share the operation of Apps on smart phones. For example, depending on short-range connection of the Bluetooth, wearers of smart watches can set their own address books via operation on smart phones. The stored data can simplify the operation of users and make a connection with family in real time. The smart watch oriented to children has the main call function to protect their safety. In addition, many wearables especially smart watches have taken a step into e-payment. NFC of newest wearables can be used as transportation card and support partial payment (Ondrus & Pigneur, 2007). Although many giant companies have contained e-payment function in their products, people show worries about security of their bank account based on the study (Yoon et al., 2015). For the property security, transmitted data need to be protected with high security level of encryption and identification. With more advanced technology of data protection, e-payment may provide convenience with larger group of users.

Apart from users, big data analytics can generate business value for companies. Supposing users give permission to companies of wearables to access partial data, wearable companies may improve efficiency by finding the interest and needs of users based on data analytics. A project report of Federal Trade Commission in the United States ('Mobile Device Tracking', 2014) has shown an increase of companies which aim to combine the stored data of users with external information to generate profiles of customers. Although privilege has to be limited for privacy, it cannot be denied that the data analytics can provide companies with a better understanding of what their like and gain insight of market. From this perspective, companies can provide better service to customers based on the interest of them. Moreover, it can stimulate the creation which is suitable for different groups of users. Based on the different characteristics of customers, different types of

devices with customized functions can be introduced to different groups of people. From the perspective of industry, smart wearables can realize remote guidance and provide stronger safeguards (Realwear, 2018)

As one of the main functions, smart wearable devices collect real-time health index of wearers. The health index stored in the devices can record a visualized change of physical status and lead to a healthier lifestyle. For example, Fitbit, as a American company famous for its activity trackers and wearable devices, introduced its products with the main functions of activity recording, sleeping monitoring, smart track and so on. According to the report on Smart Wearable Technologies and Solutions (Wang and Wang, 2017), health care and intelligence may be the mainstream of development in smart wearable devices. Based on stored data, smart wearable device can calculate user's activity and analyse the diet index or physical status. Cardiogram (2018) has estimated two trillion measurements will be produced by the wearable devices and cardiogram on the devices can detect diabetes with 85% accuracy by monitoring heart rate on wearables (Aouad, 2018). By analysing the data, it will send a warning notice if heart rate is too high or disordered. The data analytics not only illustrates the present status, but also contains function of diseases prevention. Based on the study of Yoon (2015), user experience designers show expectation in health prevention of wearables. System of wearables analyses the data of activity trailing and concludes the change of users' life quality. Chan et al (2012) have expatiated the inclination of disease resulting from the signs can be avoided by carrying out corresponding therapy. For example, degree° of Cosinuss is in-ear wearable providing real-time temperatures and can send messages to their parent if the temperatures of their children increase rapidly, which can prevent aggravation of fever and help children get timely treatment. And according to a new on Wareable.com (2018), L'Oreal has introduced a new wearable "My Skin Track UV" recently and it can measure the exposure data of UVA and UVB on users. And NFC will be used to share the data and power is supplied by solar energy. The exposure data and analysis in the wearable device can reflect the real-time UV and remind people of long-time direct exposure. As the devices step into health care, they are expected to collect more accurate data for health monitoring. And doctors can diagnose and complete telemedicine in a long distance based on data and data analytics (Zheng, 2017). Based on the data and its analytics, wearers can enjoy a more scientific lifestyle and may prevent themselves from diseases through portable devices.

Although progress of technology can be seen in the area, existing limitations may impede the development of wearable industry. Challenges like anti-interference ability of sensors and weak power sustainability still exist (An et al., 2017). With the development of data analytics and sensors, the quality of data collected from wearables may be more accurate and concise to support the long-distance diagnosis. A low-cost and convenient treatment can provide to people (Zheng, 2007). In general, big data and data analytics of wearables have provided benefits to the innovation of wearable device industry.

4 ETHICAL PROBLEMS IN WEARABLE DEVICES

Although the market needs and financial benefits stimulate the growth of the industry, some ethical problems are triggered with the use of big data and data analytics in wearable devices. The inappropriate use of data or invisible data attack may not only cause harassment to customers, but also pose a threat to property or safety of users. In this paper, ethical problems in wearable devices will be mainly concluded in risk management, system vulnerabilities and potential attack, misused data and neglect of data safety.

4.1 Risk Management of Wearables

Risk evaluation and prediction of wearables should be refined as the development of functions. HMT-1 of Realwear (2018) has functions dust tight, water and drop proof. The risk prevention functions can provide support for industry and safeguards for users in work. The risk profiling system introduced by Fugini et al., (2009) has shown realization of risk management and control. According to their research, data about the security will be defined using SOAP and alarms can be sent to users in real time. However, the improvement and popularization of risk prevention have to be supported by refining the risk profiling systems in wearables.

4.2 System Vulnerabilities and Potential Attack

In the era of big data, the privacy problem is mainly connected with the data leakage. Although people have improved their awareness of data protection, data leakage happened frequently in different systems of areas ranging from commercial companies to bank system. As for wearables, the data mainly cover sensitive health indexes of users, so the leakage of the information may cause different degree of harm to wearers. Moreover, the system vulnerabilities can be found on wearables. According to report of HP (2015), smart watch shows its vulnerabilities in insufficient authentication, lack of transport encryption, insecure cloud interface and so on. Attackers can get private information and telephone record of wearers without permission via Bluetooth, WIFI or password cracking. According to case study on device (Do et al., 2016), if USB debugging of Android is turned on, wearables may be cracked by connection to a machine controlled by hackers. Furthermore, Baggili et al., (2015) have conducted experiment on different brands of smart watch and demonstrated large amount of data in wearables can be exploited if attackers gain root access.

The system vulnerabilities may be exploited by hackers. Some researchers tested that the front door of wearables can be cracked. A study on the smart watch (Song et al., 2015) demonstrates PIN code can be deduced by the motion sensor information of wearables. Therefore, if attackers know the layout of keyboard, gyroscope sensor and accelerator can leak the action of hand movement. The PIN code can be calculated by attackers. In addition, Wang et al. (2016) described two typical attack models and recovery ability of wearable device. Sniffing attack is based on a sniffer and internal attack is based on malware App. Attackers can find sequence of PIN code via Bluetooth or wireless Internet.

Karakaya et al., (2016) have figured out that malwares set on smart watch can get access to the data on phones. Fortinet research packet can be sent by attackers via Bluetooth and the wearable data will be attacked and recorded automatically. And PC will also be infected through synchronization. The research shows that malware attack poses threat for wearables in a long distance (Smith, 2015). Data leakage not only involves the violence of privacy, but also poses threat of lives. Barnaby jack, a famous hacker and ethical cyber expert, had a stimulation demonstration to crack ATM and pacemakers (Wang, 2016). By cracking system, pacemakers can pose a threat to patients' lives. The vulnerabilities on smart wearables have a high possibility of being attacked. Data leakage may be happened in silence leading to loss of property or even endangering the lives. In order to ensure the safety of users, more researches have to be completed.

4.3 Misused Data

Since data contains business value, misused data may cause bad influence on customers. Report from Federal Trade Commission ('Mobile Device Tracking', 2014) has figured out some companies have analysed browsing history records and information of geo-location. These data may be sold for commercial profits and lead to loss of users. The report blamed some companies of mobile devices have distorted the fact that they did not comply with privacy requirement collecting data of particular person. As data on wearable devices mainly focus on health information of wearers, the data may be sold for commercial profits. The share of data between companies has violated customers' privacy as well as human rights. Therefore, more measures should be considered to reduce the cases.

4.4 Neglect of Data Safety and Privacy

Karakaya et al., (2016) consider manufactures are aiming at expanding multifunction and growing capabilities, but data safety will be important as the data cover more sensitive information. Since the smart wearable device industry is in the process of development, manufacturers tend to invest heavily on functions to attract customers' attentions without researches and tests on data safety of their wearables. A search about smart watch of children has been conducted by the author on the Internet. The result shows that some devices with high sales volume do not contain a formal brand and the price is cheaper compared with the well-known devices. Little information is provided concerning data safeguards. However, many customers have also neglected data safety when they chose the devices. Data safety should be paid more attentions by manufacturers as well as customers.

Sometimes, regulations of emerging products is easy to be neglected. Smart glasses have been introduced in market and support functions via mobile communication network. Since the glasses can take pictures and videos about what the users see, usage of smart glasses becomes sensitive. People should not record videos on some private occasions and it should not become the tool to monitor people around. More regulations of smart glasses have to be completed to protect privacy (Delail & Yeun, 2016). School uniforms with tracking chips has been introduced in China (Tahir, 2018). But the news has

aroused controversy in social media. Cameras embedded aims to record the movement of students in school. From another perspectives, GPS has violated privacy of students. Therefore, the management about the new smart technology usage are expected to be specified. With the emergence of new wearables, privacy should not be neglected.

5 LIMITATIONS AND SUGGESTIONS OF ETHICAL PROBLEMS IN SMART WEARABLE DEVICES

As ethical problems discussed before, limitations and suggestions have to be conducted for a more ethical smart wearable devices market with more transparency. Customers, companies, society and public legal institutions have responsibilities to solve the problems. Additionally, these six topics are under the future research direction.

5.1 Customers

Firstly, customers should strengthen their awareness of privacy and upload personal information with prudence. For example, some customers pay no attention about authorization of accessing data in users' devices when they installed a new application. Customers should attach importance to the privacy when providing a privilege. Based on the result of study (Ding, 2017), more than half of respondents have concerns over privacy of data stored on wearables. However, most respondents lack the knowledge of right measures to protect the data. Therefore, technical knowledge towards data protection is a weak point for users. Upgrading antivirus software and patching their systems provide stronger safeguards for wearers. With the development of advanced technology, people have to increase knowledge to protect safety of their information. Wearers of smart glass should not only protection their own privacy, but also respect others' sensitive information when they wear the devices.

5.2 Companies

Wearable companies should take on more responsibilities rather than producing devices only. Considering the eight principles about private information set by OECD, principles in Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data can be applied to companies of smart wearables.

Collection Limitation Principle (Werle & Palm, 2009) means that the smart wearable companies should get permission of wearers to access their private data before using the data. And the means of accessing data have to be lawful.

Use Limitation Principle (Werle & Palm, 2009) illustrates the data are not permitted to use for other aims. Since the data in wearable mainly are related to users' health indexes, the data leakage may cause serious problems as the technology of wearables is developed further. Therefore, companies should not share the data without the authorization of customers or sell data for commercial profits.

Security Safeguards Principle of the guidelines (Werle & Palm, 2009) has demonstrated that smart wearable companies should protect personal information from other illegal access from hackers. Therefore, anti-virus software should be further researched and developed. As mentioned in previous part, system vulnerabilities may pose threat to users and companies cannot cut the cost of data protection for profit purpose.

Openness principle (Werle & Palm, 2009) illustrates usage of data should be publicized. The companies should make an announcement to detail the usage of private data at regular intervals. If the data keep no transparency, customers do not have an access to know the usage of data. Openness principle requires companies to take the responsibilities and use private data in a lawful and fair way.

5.3 Society

With the development of advanced technology, more public speeches or online lessons can be provided to improve technical knowledge for different groups of people. Since smart wearables have developed for several years, different brands of wearables are introduced in the market. Therefore, stronger supervisions can be carried out by organizations. Food and Drug Administration has released the regulations on wearables and guaranteed digital health (Dolan, 2015). Management of wearables requires supervisions of organizations and leading guidance.

Standard of smart wearables is another challenge for the industry. Organizations have instituted standard systems of RFID technology, but challenges still exist in setup of certain systems considering of industry development. For example, China has dedicated to institute the RFID standards which can support the industry development and ensure the

security (SZCANBO, 2018). According to the news on SZCANBO, the industry chain of RFID has been built in China. In terms of low frequency market and UHF, China still faces challenges. The actual development of industry is close connected with standards. Therefore, research will still be the focus. Furthermore, the smart industry is able to provide a healthier lifestyle and a great influence on health care system, thus investment or other forms of support from society may stimulate the innovation of smart wearables.

5.4 Standardization

According to Aubert (2011), some of ethical issues can be minimized by the use of standardization, such as in RFID technologies. When designing RFID, users' data can be carefully handled to ensure privacy can be maintained. Additional effort can be made to ensure careful handling of users' data, such as anonymized status. Standardizations in regulations, use of smart wearables, technical requirements, choices of materials for wearables and the code of practices can be highlighted, so that ethics of smart wearables can be maintained.

5.5 Risk Management

Risk management is useful to minimize ethical issues as follows. First, a full risk management should be in smart wearable devices for both hardware and software, so that it can protect patients from attacks, vulnerability, misused data or neglect of data safety. Second, risk management can be used in the hardware and service design and be fully tested, in order to ensure sensitive data can be safe from the data leak or misuses. This can blend with standardization to ensure all technologies adopted smart wearables have high quality and guarantee of services. Third, the connection to the online social networks should be carefully monitored and managed. We should prevent sensitive data to be uploaded and exposed to the social networks with more levels of authorization and privacy to be implemented and enhanced for smart wearables.

5.6 Benefits of adopting this research

Academia can help practitioners, medical staff and health scientists by promoting the importance of smart wearables. Universities can collaborate further with industry, hospitals and education sector so that the general public can become more aware of its issues, challenges, latest outputs, as well as the benefits of using smart wearables. The general public and students can be better educated for the proper uses of smart wearable and training requirements.

6 CONCLUSIONS

In this paper, different aspects of smart wearable devices have been overviewed. Although big data and big data analysis have provided convenience and heathier lifestyle for users, it also triggers ethical problems. From the perspective of personal data, system vulnerabilities discovered by experiments might be accessed by hackers (Do et al., 2016). In future, data leakage of health data is possible to have more serious consequences as the functions of wearables advance. Misused data mainly resulting from the unethical sales of data may cause annoyance of advertisement or other danger. In addition, companies of wearables put more attention to functions at the primary stage rather than safeguards (Do et al., 2016). Based on the problems, some suggestions are provided from perspectives of customers, wearable companies and society. Although the growth of smart wearable trend fluctuates, smart wearable devices still have great potential in sports and health care (Wang and Wang, 2017). With development in wearables, more innovation may be applied to the devices for solving the constraints. And smart wearable devices can provide a healthier lifestyle for people.

REFERENCES

An, B. W., Shin. J. H., Kim, S. Y., Kim, J., Ji, S., Park, J., Lee, Y., Jang, J., Cho, E., Jo, S., & Park, J. (2017). Smart Sensor Systems for Wearable Electronic Devices. *Polymers*, 9(8).

Aouad, A. (2018, February 10). Digital Health Briefing: Cardiogram uses Apple Watches to detect diabetes-Kansas. physicians weigh in on telehealth bill-GE to bring health solution to the Olympics. *Yahoo*. Retrieved from https://uk.news.yahoo.com/digital-health-briefing-cardiogram-uses-183500592.html

Aubert, H. (2011). RFID technology for human implant devices. Comptes Rendus Physique, 12(7), 675-683.

Baggili, I. , Oduro, J. , Breitinger, F. , & Mcgee, G. (2015). Watch What You Wear: Preliminary Forensic Analysis of Smart Watches. *International Conference on Availability*. IEEE.

Chan, M., Fourniols, J. Y., Escriba, C., & Campo, E. (2012). Smart wearable systems: current status and future challenges. *Artificial Intelligence in Medicine*, 56(3), pp.137-156.

Chen, J. , Chen, Y. , Du, X. , Li, C. , Lu, J. , & Zhao, S. , et al. (2013). Big data challenge: a data management perspective. *Frontiers of Computer Science*, 7(2), pp.157-164.

China's RFID standards are coming soon. (2018, May 10). *SZCANBO*. Retrieved from http://www.szcanbo.com/en/article-76629-104746.html

Smith, C. (2015, October 21). Hackers can invade a PC with a 10-second attack on a Fitbit. *BGR*. Retrieved from https://bgr.com/2015/10/21/fitbit-malware-hack-pc

Cosinuss°. (2018). Retrieved from https://www.cosinuss.com

Delail, B. A. , & Yeun, C. Y. (2016). Recent advances of smart glass application security and privacy. *Internet Technology & Secured Transactions*. IEEE.

Ding, X. N. (2017). 'Research on Mobile Intelligent Terminal Security Threat and Protection (in Chinese)'. *Digital Technology and Application*(1), pp. 192-193.

Do, Q., Martini, B., & Choo, K. K. R. (2016). Is the data on your wearable device secure? an android wear smartwatch case study. *Software Practice & Experience, 47*(3).

Dolan, B. (2015, January 16). FDA clarifies the line between wellness and regulated medical devices. *Mobihealthnews*. Retrieved from https://www.mobihealthnews.com/39775/fda-clarifies-the-line-between-wellness-and-regulated-medical-devices

Dong, S., Bai M., & Yan, H. M. (2016). Research on influence on safety and efficiency of medical devices induced by RFID system. *China Medical Equipment.* 13(1), pp.126-128.

Edwards, B. (2013, February 18). Evolution of the smartwatch. *PCWorld*. Retrieved from https://www.pcworld.com/article/2028545/evolution-of-the-smartwatch.html#slide9

Filip. (2017). *Germany Bans Smartwatches For Kids*[online]. Retrieved from http://www.nextpowerup.com/news/39786/germany-bans-smartwatches-for-kids/

Fitbit. (2018). Retrieved from http://www. fitbit.com/cn/home

Fugini, M. , Conti, G. M. , Rizzo, F. , Raibulet, C. , & Ubezio, L. . (2009). Wearable Services in Risk Management. *IEEE/WIC/ACM International Joint Conference on Web Intelligence & Intelligent Agent Technology*. IEEE Computer Society.

'Google Glass'. (2018). Retrieved from https://www.techopedia.com/definition/28524/google-glass

'History and development trend of smart bracelet (in Chinese)'. (2017, January 3). *Zaker*. Retrieved from http://www.myzaker.com/article/586b6c451bc8e0ff0800000a/

'Internet of Things Security Study: Smartwatches'. (2015). *Federal Trade Commission*. Retrieved from https://www.ftc.gov/system/files/documents/public_comments/2015/10/00050-98093.pdf

Jayalath, S., & Abhayasinghe, N. (2013, April). A gyroscopic data based pedometer algorithm. *International Conference on Computer Science & Education*.

Karakaya, M., Bostan, A., & Gökçay, E. (2016). *How Secure is Your Smart Watch?*. Proceedings of 9th International Conference on Information Security and Cryptology (ISCTURKEY 2016), pp.138-145.

Kastrenakes, J. (2014, June 25). Samsung Gear Live and LG G Watch available to order today. *The verge*. Retrieved from https://www.theverge.com/2014/6/25/5841436/samsung- android-wear-smartwatch-unveiled

Li, D. R., Yao, Y., & Shao, Z. F. (2014). Big Data in Smart City. *GEOMATICS AND INFORMATION. SCIENCE OF WUHAN UNIVERS*, 39(6), pp. 631-640.

Mawston, N. (2018, November 2). Global Smartwatch shipments soar to 10 Million in Q3 2018. *Strategy Analytics*. Retrieved from https://www.strategyanalytics.com/strategy-analytics/blogs/devices/wearables/wearables/2018/11/02/global-smartwatch-shipments-soar-to-10-million-in-q3-2018

Mukhopadhyay, S. C. (2015). Wearable sensors for human activity monitoring: A review. IEEE sensors journal, 15(3), 1321-1330.

Ondrus, J., & Pigneur, Y. (2007). An Assessment of NFC for Future Mobile Payment Systems. *International Conference on the Management of Mobile Business*. IEEE Computer Society.

Realwear. (2018). Introducing HMT-1Z1. Retrieved from https://www.realwear.com/products/hmt-1z1

RFID standards. (2019, February 17). *Impinj*. Retrieved from https://www.impinj.com/about-rfid/rfid-standards/

Wang, C. , Guo, X. , Wang, Y. , Chen, Y. , & Liu, B. (2016). Friend or foe?:your wearable devices reveal your personal pin.

Wang, Q. (2016). Research on Information Security Issue of Wearable Device. *Information Research*(3), pp.122-124.

Wang, Y., & Wang, J. W. (2017). Smart Wearable Technologies and Solutions. *Electronic Engineering & Product World for Engineering Managers & Designers*, 24(9), pp.14-20.

Werle, E. , & Palm, D . (2009). Guidelines governing the protection of privacy and transborder flows of personal data. *IEEE Technology & Society Magazine*, 2(2), pp.27-28.

The Website: www.chyxx.com, accessed on February 19, 2019

The Website: Zhiyan.org, accessed on February 19, 2019.

Wu, F., Li, X. , Xu, L. , Kumari, S. , Karuppiah, M. , & Shen, J. (2017). A lightweight and privacy-preserving mutual authentication scheme for wearable devices assisted by cloud server. *Computers & Electrical Engineering*, *S0045790617308984*.

Sawh, M. (2018, November 14). L'Oréal launches My Skin Track UV to keep you safe in the sun and out of the smog. *Wareable*. Retrieved from https://www.wareable.com/wearable-tech/loreal-my-skin-track-uv-price-release-date-specs-6723

'Spring Privacy Series: Mobile Device Tracking'. (2014, February 19). *Federal Trade Commission*. Retrieved from https://www.ftc.gov/news-events/events-calendar/2014/02/spring-privacy-series-mobile-device-tracking

Song, C. G., Liu, J. W., Wu, Q. H., & Guan, Z. Y. (2015). 'New Attack Based on Smartwatch Motion Sensors and the Protection Method Research'. *Journal on Communications*, 36(s1), 235-242.

Tahir, T. (2018, December 24). CLASSROOM MONITOR China puts TRACKING CHIPS in school uniforms to watch pupils every move. *The Sun.* Retrieved from https://www.thesun.co.uk/news/8056887/china-tracking-chips-school-uniforms/

Yoon, H., Shin, D. H., & Kim, H., (2015). *Health Information Tailoring and Data Privacy in a Smart Watch as a Preventive Health Tool*. Springer International Publishing.

Zheng, J. W. , Zhang, Z. B. , Wu, T. H. , & Zhang, Y. (2007). A wearable mobihealth care system supporting real-time. diagnosis and alarm. *Medical & Biological Engineering & Computing*, 45(9), pp.877-885.